Key Generation Method For Communication Session Encryption And Authentication System

ABSTRACT

An interactive mutual authentication protocol, which does not allow shared secrets to pass through untrusted communication media, integrates an encryption key management system into the authentication protocol. The server provides ephemeral encryption keys in response to a request during a Session Random Key (SRK) initiation interval. SRK is provided for all sessions initiated in the SRK initiation interval. A set of ephemeral intermediate Data Random Keys (DRK) is associated with each request. A message carrying the SRK is sent to the requestor. A response from the requestor includes a shared parameter encrypted using the SRK verifying receipt of the SRK. After verifying receipt of the SRK at the requestor, at least one message is sent by the server carrying an encrypted version of one of said set of ephemeral intermediate DRK to be accepted as an encryption key for the session.